

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail in an envelope addressed to:

ASSISTANT COMMISSIONER OF PATENTS
WASHINGTON, DC 20231

bearing Label Number EE 651 410 111 US and mailed

Ira Richardson

Print Name

10/12/00


Signature

Patent

Inventors: Richard Alan Dayan
Joseph Wayne Freeman
Steven Dale Goodman
Joseph Michael Pennisi
Randall Scott Springfield
James Peter Ward

Title: **Method and System for Booting Up a Computer System
in a Secure Fashion**

RPS9 2000 0066

METHOD AND SYSTEM FOR BOOTING UP A COMPUTER SYSTEM IN A SECURE FASHION

FIELD OF INVENTION

The present invention relates generally to the field of computer security and particularly a method and system for booting up a computer system in a secure fashion.

5

BACKGROUND OF THE INVENTION

Personal computer systems in general have attained widespread use for providing computer power to many segments of today's modern society. Personal computer systems can usually be defined as a desktop, floor standing, or portable microcomputer that comprises a system unit having a single system processor and associated volatile and non-volatile memory. Figure 1 is an example of a typical personal computer system 10. The personal computer system 10 typically includes an associated display monitor 11, a keyboard 12, one or more diskette drives 13, an associated printer 14, and a hard drive (not shown).

With the phenomenal growth and use of personal computers in the world in recent years, more and more data or information is being collected and retained or stored in such systems. A lot of this data is sensitive in nature. In the wrong hands, data could become embarrassing to individuals, a company could lose a competitive edge, or sensitive data could be used to force payment for silence or lead to physical violence against individuals.

As more users recognize the sensitive nature of data and its value, the more it becomes desirable to protect against such misuse.

To protect themselves and the persons associated with the stored data, users are requiring the incorporation of security and integrity features into the personal computers that

they purchase. Consequently, as security requirements for personal computer systems continue to become more sophisticated, the addition of cryptography hardware will become mandatory for some market segments. Other market segments will be unwilling to pay for the increased system cost resulting from the addition of what is perceived to be unneeded hardware. This dichotomy requires personal computer vendors to manufacture and maintain different system configuration whose only difference is the presence or absence of the cryptography hardware. Alternatively, some vendors may choose to manufacture a single system whose security features can be upgraded by adding a hardware module or card. In the latter case, some protection is needed to ensure that sensitive data (i.e., encryption keys) on the card, along with the secrets that they protect, are not compromised if the card is moved between systems.

Accordingly, what is needed is a method and system for determining whether a security card has been added/removed from a computer system thereby allowing the computer system to boot up in a more secure fashion. The method and system should be simple, cost effective and capable of being easily adapted to current technology. The present invention addresses such a need.

SUMMARY OF THE INVENTION

A method and system for booting up a computer system in a secure fashion is disclosed. The method and system comprise determining the presence of a security feature element during an initialization of the computer system wherein the security feature element includes a public key and a corresponding private key, storing a portion of the public key in a nonvolatile memory within the computer system if the security feature element is present

and utilizing an algorithm to determine the presence of the security feature element prior to a subsequent boot-up of the computer system.

Through the use of the present invention, a computer system is capable of being booted up whereby the computer system determines if a security feature element was previously present in the system. If a security feature element was previously present in the computer system, any stored keys, along with the secrets that they protect, are prevented from being compromised. It is also an object of the present invention to preclude the system from compromising any keys and associated secrets if a security feature element in the system was not previously present in the system.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is an example of a typical personal computer system.

Figure 2 is a high level flowchart of the method in accordance with the present invention.

Figure 3 schematically shows the insertion of the security card into a computer system.

Figure 4 is a flowchart of the algorithm in accordance with the present invention.

Figure 5 is an example of a comparison chart utilized by the method and system in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention provides a method and system for booting up a computer system in a secure fashion. The following description is presented to enable one of ordinary

skill in the art to make and use the invention and is provided in the context of a patent application and its requirements. Various modifications to the preferred embodiment will be readily apparent to those skilled in the art and the generic principles herein may be applied to other embodiments. Thus, the present invention is not intended to be limited to the embodiments shown but is to be accorded the widest scope consistent with the principles and features described herein.

The present invention is presented in the context of a preferred embodiment. The preferred embodiment of the present invention is a method and system for booting up a computer system in a secure fashion. Essentially, the method and system in accordance with the present invention verifies whether the public key that was previously installed within the computer system (via a security feature element) has not changed since the installation of the key. This is achieved through the utilization of an algorithm contained within the basic input/output system ("BIOS") image. Accordingly, through the use of the algorithm, the computer system can be securely booted up whereby the public/private key pair of the security feature element, along with the secrets that they protect, are not compromised.

The security feature element that is used in conjunction with the method and system in accordance with the present invention preferably comprises a security card. This card adds support to the computer system for tamper detection, temperature monitoring, voltage status reporting, Alert on Lan II signal collection, and Secure Client signature generation.

The security card also includes nonvolatile storage for a hardware platform key pair, wherein the key pair includes a public key and a corresponding private key. The public/private key pair is subsequently utilized in conjunction with corresponding

public/private key pairs within the computer system to unlock certain secret components of the computer system. Consequently, the utilization of the keys in an unauthorized manner must be avoided. Accordingly, the method in accordance with the present invention prevents such unauthorized use when a security card is moved from one system to another.

5 Although the above described security card is disclosed in the context of including a single public/private key pair, one of ordinary skill in the art will readily recognize that the security card in accordance with the present invention could include more than one public/private key pair while remaining within the spirit and scope of the present invention.

To further understand the method in accordance with the present invention, please refer now to Figure 2. Figure 2 is a high level flowchart of the method in accordance with the present invention. First, a determination is made as to the presence of a security feature element during an initialization of a computer system, via step 50. Preferably, the security feature element comprises a security card that includes nonvolatile storage for a hardware platform key pair, wherein the key pair includes a public key and a corresponding private key. Next, a portion of the public key is stored in a nonvolatile memory within the computer system if the security feature element is present, via step 52. Preferably, during the first-time initialization, a portion of the public key contained on the security card is provided to the BIOS software whereby the BIOS software stores the portion of the public key into an Electrical Erasable Programmable Read Only Memory (EEPROM) contained within the computer system. Finally, an algorithm is utilized to determine the presence of the associated security card prior to each subsequent boot-up of the computer system, via step 54. Preferably, the BIOS software utilizes a binding algorithm during each subsequent

Power-On-Self-Test (“POST”) procedure to determine the presence of the security card prior to relinquishing control of the operating system.

The POST routines provide an extensive check for system integrity. These include for example, surveying the system configuration, performing sanity checks on system hardware, issuing diagnostic signals, etc. The BIOS software contains routines for interfacing to key peripherals, for interrupt handling, and so forth. The BIOS software itself is normally packaged in nonvolatile memory with other key pieces of software and management routines, as well as a pointer to launch the computer into the operating system software. In accordance with the present invention, as long as the correct security card is present during the POST routine, the computer system boots up in a normal fashion.

For a better understanding of the present invention, please refer now to Figure 3. Figure 3 schematically shows the insertion of the security card 130 in accordance with the present invention into a computer system 155. The computer system 155 includes a CD-ROM 100, a floppy drive 105, a nonvolatile memory 115, a system board 120, a central processing unit (CPU) 125 and the security card 130. The security card 130 includes a microcontroller 135 which includes a small amount of nonvolatile memory 140 which contains a hardware platform key pair wherein the hardware platform key pair comprises a public key/private key pair. The nonvolatile memory also includes storage for a plurality of additional key pairs. The computer system 155 also includes a keyboard 145, BIOS modules 146 and random access memory (RAM) 150. In accordance with the present invention, each POST of the computer system utilizes a binding algorithm to ensure that the security card 130 has not been subjected to an unauthorized tamper event.

5

It should be noted that the above described computer system is only an example of a system in which the present invention could be implemented. Consequently, one of ordinary skill in the art will readily recognize that the present invention could be implemented in a wide variety of computer systems while remaining within the spirit and scope of the present invention.

10

For a further understanding of the algorithm in accordance with the present invention, please refer to Figure 4. Figure 4 is a flowchart of the POST binding algorithm in accordance with the present invention. First, a determination is made as to whether a card is present, via step 200. If there is no card present, a determination is made as to whether a card was previously installed in the system and thus removed, via step 202. If a card wasn't previously installed then the system boots up normally, via step 216. If a card was previously installed and therefore removed, the portion of the public key contained in the EEPROM is cleared, via step 210. Preferably, a POST error is then issued that indicates that a card was previously installed in the system and the card has subsequently been removed i.e., some secret information related to the computer system may have been compromised. The user will then be prompted to provide some type of administrator authentication (i.e. administrator level password) to proceed with the boot-up process, via step 212. If the administrator authentication is not properly entered, the system will not boot-up, via step 214. If the administrator authentication is properly entered, the system will boot-up, via step 216.

20

Referring back to step 200, if a card is present, a determination is made as to whether the system has been tampered with, via step 204. Preferably, this step involves the utilization of a cover tamper switch and a tamper latch, wherein the tamper latch is used to

indicate whether the system cover was opened. It should be noted that the tamper latch could be equipped to be triggered based on a variety of tamper events i.e. power being removed from the security element, etc. If the system has not been tampered with, the system boots up normally, via step 216. If the system has been tampered with, a determination is made as to whether the card has been added to the system, via step 206. Preferably, the binding algorithm is equipped with logic that is capable of determining whether or not a card is supposed to be present within the system based on the completion of a previous POST sequence.

Consequently, if the card is a feature that has been added to the system, the portion of the public keys of the previously installed card that are contained in the EEPROM are cleared, via step 210. The user will then be prompted to provide some type of administrator authentication to proceed with the boot-up process, via step 212. If the administrator authentication is not properly entered, the system will not boot-up, via step 214. If the administrator authentication is properly entered, the system will boot-up, via step 216.

Referring back to step 206, if the card is not a feature that has been added to the system, the portion of the public key is read from the card and is compared with the portion of the public key contained in the EEPROM, via step 208. Preferably, this step involves the utilization of a comparison chart such as the one shown in Figure 5. If the keys match (i.e. if the test result is "pass"), the system boots up normally, via step 216. If the keys don't match (i.e. if the test result is "fail"), the user is notified and the keys stored on the card as well as the keys contained in the EEPROM are cleared, via step 210. The user will then be prompted to provide some type of administrator authentication to proceed with the boot-up process, via step 212. If the administrator authentication is not properly entered, the system

will not boot-up, via step 214. If the administrator authentication is properly entered, the system will boot-up, via step 216.

An additional feature of the method and system in accordance with the present invention is associated with the unlikely event that a card is installed while power is being applied to the system. If a card is installed while power is being applied to the system, the card will assert a signal to force a reset of the system. This is done in order to force the system to execute the POST sequence before any malicious activity can occur on the card to clear evidence of a tamper event. This will appear to the system BIOS as a cold boot and the tamper latch will be activated to indicate a tamper event.

Although the present invention has been described in accordance with the embodiments shown, one of ordinary skill in the art will readily recognize that there could be variations to the embodiments and those variations would be within the spirit and scope of the present invention. Accordingly, many modifications may be made by one of ordinary skill in the art without departing from the spirit and scope of the appended claims.